



# DEFENDERBOX Funktionsumfang

## Modul 3

### INTERNE ANGREIFBARKEIT

#### Internes Pentesting

##### Asset Discovery

##### Network Segmentation Analysis

##### Information Gathering

Ports	HTTP-Header	Webanwendungen	SNMP v1/v2/v3	mDNS
SSH	VNC	RDP	Telnet	

##### CVE Scanning

Ports	HTTP-Header	Webanwendungen	SNMP v1/v2/v4	SSH
WMI				

##### Credential Verification

###### Verwendung von Domänenbenutzeranmeldeinformationen

Passwort-Spraying von Azure-Cloud-Benutzern mit gängigen Passwörtern. Es besteht eine geringe Wahrscheinlichkeit, dass Konten gesperrt werden.	Überprüft den Zugriff auf Dienste und Freigaben mit lokaler Benutzerauthentifizierung (ohne Domäne).	Überprüft den Zugriff von Windows-Domänenbenutzern durch Authentifizierung mit Anmeldeinformationen gegenüber dem SMB-Service, der auf dem Windows Domain Controller läuft.	Ermöglicht das Passwort-Spraying von Domänenbenutzern mit gängigen Passwörtern. Standardmäßig wird ein Benutzer nur zweimal alle 60 Minuten versucht.
--	--	---	---

##### Service Brutforce

###### Durch unzähliges Ausprobieren von Benutzernamen und Passwort-Kombinationen versucht NodeZero in das System einzudringen.

SSH	Telnet	RDP	MySQL	Mongo DB
MS SQL	Redis	Maria DB	PostgreSQL	"HTTP Basic Auth/ HTTP Web Forms"
FTP	SNMP	SMB		

##### Service Discovery

In der Diensterkennungs-Phase testet NodeZero die gefundenen Services auf spezifische, häufig vorkommende Sicherheitslücken, die durch eine falsche Konfiguration entstehen.

Dabei werden unter anderem Authentifizierungsverfahren, die Verschlüsselung von Verbindungen oder Ausführungs- und Zugriffsrechte unter die Lupe genommen.

SSH	Telnet	DNS	MySQL	Mongo DB
MS SQL	HTTP	SSL/TSL	LDAP	SNMP v1/v2/v4
HTTP Header	FTP	SMTP	SMB	

##### Footprinting der Anwendungsumgebung

Insbesondere Versionsnummern stellen für Angreifer eine wertvolle Information dar. NodeZero untersucht, welche Technologien die Webseite in einem HTTP-Header, einem Cookie oder im Code preisgibt.

Das Footprinting umfasst Programmiersprachen, Content Management Systeme, Webserver, Frameworks oder Libraries. Eine eindeutige Bewertung gibt an, wie kritisch die ermöglichte Detektion der jeweiligen Technologie einzuschätzen ist.

für Angreifer sichtbare Technologien aufdecken

Scan der HTTP-Header, Cookies und des Webseiten-Codes